Procedure #	Document Title / Approver	Effective Date	Revision # / Date
N/A	Secure System User Account Management / Technology Manager/Program Director	09/15/2017	09/28/2018

Secure System User Account Management

1.0 Purpose

The system user account management procedure operates within the GDIT TTP Information Security Program to establish management steps in the TTP information system user account lifecycle. These user account management steps ensure safeguarding of the information system and its data assets. The procedural details of this policy refer to GDIT as the corporate or primary contractor entity.

2.0 Scope

The procedure applies to:

- All GDIT TTP employees, contractors, and third parties (collectively, users) whose roles are to manage or administer the access or other use of the TTP information system.

3.0 Procedure

This section presents an overview of the main process steps for secure TTP system account management for all users. The process moves from onboarding through monitoring, review, and offboarding.
For account management implementation notes, please see the work aid, TTP User Account Management.

Step	HFPP Partner	Other TTP Personnel Users

Step	HFPP Partner	Other TTP Personnel Users
1	ONBOARDING AND ACCESS HFPP Partner selection and approval processes are completed. Partner candidate sends formal request for HFPP membership.	ONBOARDING AND ACCESS TTP employee new hire selection and acceptance is completed. Newly-hired TTP employee completes all required corporate (primary) / subcontractor legal and related documentation. (Includes TTP PMO documentation for new staff.)
2	New Partner introduced to the Memorandum of Understanding (MOU) and Data Sharing Agreement (DSA) documents.	New TTP employee information system role and type is determined to coordinate system accesses: *Two general TTP access types identified for Admins/Developers and Analysts.*
3	Executed MOU/ DSAs stored on SharePoint.	New TTP employee completes security and related agreements (RoB & others) required for system access types.
4	Once MOU is executed: A: HFPP Partner Orientation Meeting held. B: New Partner identifies POC and additional Portal users. C: Request made for new user access to TTP Portal for new Partner.	Information system/Portal and other relevant training provided.
5	A: Meeting follow-ups held to support new Partner in completing DSA.	Once agreements/training complete, Tech Mgr. is notified. System accesses implemented for Admins/Developers and Analysts, accordingly.
6	B, C: Once IT receives new user access request for new Partner, the new Partner POC identity is verified.	*For new Admins/Developers*: System tickets opened/corporate cloud services requested for VPN access (to the TTP system).
7	Once the new Partner POC/new system user is verified through appropriate program processes, the new user system role and type is determined.	Once new TTP employee accesses established, tickets closed.
8	Add user form is created / new user registered.	

Step	HFPP Partner	Other TTP Personnel Users
9	Registration data sent to Portal, which sends to Microsoft Active Directory (AD) where the data is received/stored. Receipt of registration data triggers Portal account activation email.	
10	Portal account activation email sent to new user.	
11	New user receives Portal account activation email; clicks link to take security training and begin Symantec VIP (VIP) access process.	
12	New user presented with registration screens; proceeds through VIP access process and completes as instructed.	
13	Portal receives confirmation that VIP process is complete; presents Create Password form.	
14	New user completes Create Password form.	
15	New user data processed by AD and rejected/verified for storage and confirmation with the Portal. (If AD rejects user data, step is restarted, "Portal account activation email sent to new user.")	
16	AD approves password; sends confirmation to Portal.	
17	Secure sign-in page presented to new user.	
18	New user signs in with new password; Portal Dashboard page or Portal main menu landing page is presented. TTP system access is complete.	

Step	HFPP Partner	Other TTP Personnel Users
19	(COMMON PROCESS) ACCOUNT MONITORING AND REVIEW IT team identifies privileged and nonprivileged user accounts types and establishes a monitoring schedule for each type.	
20	Assigned IT team members review each account type on the designated schedules.	
21	IT team member documents the results of the review of user account status and takes any appropriate action, as required.	
22	OFFBOARDING AND DEACTIVATION TTP liaison to HFPP Partner receives notice of a separating Partner team member and Portal user.	OFFBOARDING AND DEACTIVATION TTP-assigned or corporate manager sends to TTP ticket system the personnel separation notice/TTP user separation request. Note 1: TTP PMO may also send separation ticket requests for both corporate (primary) and subcontr. personnel. Note 2: Corporate managers of primary TTP employees will manage all separation requests including return-of-assets, according to governing corporate policies.
23	T2/4 liaison sends a TTP user separation request to TTP ticket system and copies PMO.	
24	(COMMON PROCESS) OFFBOARDING AND DEACTIVATION Ticket assigned, with 24H timeframe prioritized. Ticket documentation requests, as possible, a completion confirmation email generated and sent to requestor and PMO.	
25	Access terminated across all system components within required timeframe. Any additional required corporate / PMO termination steps completed.	
26	Notice of closed ticket copied to requestor and PMO.	
27	PMO creates program record of emailed ticket confirmation (user account deactivation complete).	

4.0 Roles and Responsibilities

Error! Reference source not found. describes roles and responsibilities in secure user account management.

Table 1: Overview of Roles and Responsibilities

Role	Responsibility
Technology Manager	Ensures that assigned technical staff carry out their account management tasks throughout the identified user lifecycle.
PMO, TTP Task Leads/Managers	Ensures that required documentation is provided to verify fulfillment of approved procedures or protocols for secure account management.

5.0 Exceptions

Exceptions or variances to this policy must be authorized in writing by the documented approver.

6.0 Compliance

Any TTP employee or subcontractor manager, lead, or system administrator who knowingly violates or attempts to violate this policy shall be subject to disciplinary action, up to and including termination of employment.

7.0 References

The following GDIT TTP policy contains related information:

- GDIT Information Security Policy